AMENDMENTS TO THE CLAIMS

(IN FORMAT COMPLIANT WITH THE REVISED 37 CFR 1.121)

1. (CURRENTLY AMENDED) A method of ~~defining a transformation~~ transforming between an input signal and an output signal of a circuit, the method comprising the steps of:

(A) copying a plurality of symbols from a source file to a plurality of tables of said circuit;

~~(A)~~ (B) allocating said input signal among a plurality of block input signals;

~~(B)~~ (C) generating ~~establishing a plurality of transfer functions each configured to present a plurality of unique symbols as~~ a plurality of block output ~~signal~~ signals each responsive to (i) one of said block input ~~signal~~ signals and (ii) said symbols in one of said tables; and

~~(C)~~ (D) concatenating said block output signals to form said output signal of said circuit.

2. (CURRENTLY AMENDED) The method according to claim 1, wherein the step ~~(C) is~~ of concatenating comprises the sub-steps of:

concatenating said block output signals to form an intermediate result~~, the method further comprising the step of~~

~~establishing a second transfer function configured to permutate;~~ and

permutating each of a plurality of portions of said intermediate result to present said output signal.

3. (CURRENTLY AMENDED) The method according to claim 1, wherein each of said ~~transfer function is a table configured as~~ tables comprise k columns and 2^k rows, where k is a bit width of each of said block input ~~signal~~ signals and each of said ~~row~~ rows stores a unique one of said symbols.

4. (CURRENTLY AMENDED) The method according to claim ~~3~~ 1, ~~further comprising the step of extracting said plurality of symbols stored in said tables from a random source configured such that~~ wherein each of said ~~symbol~~ symbols in said source file has an approximately equal probability of appearance.

5. (CURRENTLY AMENDED) The method according to claim ~~4~~ 1, further comprising the steps of:

(i) selecting a staring point within said ~~random~~ source file to extract said symbols for a first table of said tables;

(ii) calculating a number of symbols extracted for said first ~~said~~ table; and

(iii) calculating a subsequent starting point to extract said symbols for a subsequent table of said tables based upon said starting point and said number ~~in response to steps (i) and (ii);~~

~~(iv) updating said subsequent starting point based upon said subsequent starting point and said number; and~~

~~(v) repeating step (iv) for all remaining said tables~~.

6. (CURRENTLY AMENDED) The method according to claim 5, further comprising the step of:

presenting ~~said~~ both a bit width of said block signals and said starting point external to said circuit as a cryptographic key.

7. (CURRENTLY AMENDED) The method according to claim 1, wherein ~~step (A) is allocating~~ a predetermined number of units of said input signal are allocated to ~~each~~ a plurality of said block input ~~signal~~ signals.

8. (CURRENTLY AMENDED) The method according to claim 7, ~~further comprising the step of allocating~~ wherein fewer than said predetermined number of units are allocated to one of said block input signals.

9. (CURRENTLY AMENDED) The method according to claim 1, further comprising the step of:

generating ~~establishing a counter configured to produce~~ said input signal by counting a clock signal.

10. (CURRENTLY AMENDED) The method according to claim 9, further comprising the steps of:

generating ~~duplicating said counter and said plurality of transfer functions to produce~~ a plurality of said output signals in response to a plurality of said countings; and

concatenating said plurality of output signals to present a second output signal.

11. (CURRENTLY AMENDED) An information recording medium for use in a computer to define a transformation between an input signal and an output signal, the information recording medium recording a computer program that is readable and executable by the computer, the computer program comprising the steps of:

(A) copying a plurality of symbols from a source file to a plurality of tables;

~~(A)~~ (B) allocating said input signal among a plurality of block input signals;

~~(B)~~ (C) generating ~~establishing a plurality of transfer functions each configured to present a plurality of unique symbols~~

~~as~~ a plurality of block output ~~signal~~ signals each responsive to (i) one of said block input ~~signal~~ signals and (ii) said symbols in one of said tables; and

~~(C)~~ (D) concatenating said block output signals to form said output signal.

12. (CURRENTLY AMENDED) The ~~computer program~~ information recording medium according to claim 11, wherein the step ~~(C) is~~ of concatenating in said computer program comprises the sub-steps of:

concatenating said block output signals to form an intermediate result~~, the computer program further comprising the step of establishing a second transfer function configured to permutate~~; and

permutating each of a plurality of portions of said intermediate result to present said output signal.

13. (CURRENTLY AMENDED) The ~~computer program~~ information recording medium according to claim 11, wherein each of said ~~transfer function is a table configured as~~ tables comprise k columns and 2^k rows, where k is a bit width of each of said block input ~~signal~~ signals and each of said ~~row~~ rows stores one of said symbols.

14. (CURRENTLY AMENDED) The ~~computer program~~ information recording medium according to claim ~~13~~ 11, ~~further comprising the step of extracting said plurality of symbols stored in said tables from a random source configured such that~~ wherein each of said ~~symbol~~ symbols in said source file has an approximately equal probability of appearance.

15. (CURRENTLY AMENDED) The ~~computer program~~ information recording medium according to claim ~~14~~ 11, wherein said computer program further comprising the steps of:

(i) selecting a staring point within said ~~random~~ source file to extract said symbols for a first table of said tables;

(ii) calculating a number of symbols extracted for said first ~~said~~ table; and

(iii) calculating a subsequent starting point to extract said symbols for a subsequent table of said tables based upon said starting point and said number ~~in response to steps (i) and (ii);~~

~~(iv) updating said subsequent starting point based upon said subsequent starting point and said number; and~~

~~(v) repeating step (iv) for all remaining said tables~~.

16. (CURRENTLY AMENDED) The ~~computer program~~ information recording medium according to claim 15, wherein said computer program further comprising the step of:

presenting ~~said~~ both a bit width of said block signals and said starting point external to said computer as a cryptographic key.

17. (CURRENTLY AMENDED) The ~~computer program~~ information recording medium according to claim 11, wherein ~~step (A) is allocating~~ said computer program allocates a predetermined number of units of said input signal to ~~each~~ a plurality of said block input ~~signal~~ signals.

18. (CURRENTLY AMENDED) The ~~computer program~~ information recording medium according to claim 17, ~~further comprising the step of allocating~~ wherein said computer program allocates fewer than said predetermined number of units to one of said block input signals.

19. (CURRENTLY AMENDED) The ~~computer program~~ information recording medium according to claim 11, wherein said computer program further comprising the step of:

generating ~~establishing a counter configured to produce~~ said input signal by counting a clock signal.

20. (CURRENTLY AMENDED) A circuit comprising:

means for copying a plurality of symbols from a source file to a plurality of tables;

means for allocating an input signal among a plurality of block input signals;

means for generating ~~establishing a plurality of transfer functions each configured to present a plurality of unique symbols as~~ a plurality of block output ~~signal~~ signals each responsive to (i) one of said block input ~~signal~~ signals and (ii) said symbols in one of said tables; and

means for concatenating said block output signals to form an output signal.